ECS 20 — Lecture 12 — Fall 2013 —5 Nov 2013

Phil Rogaway

Today:

Functions, continued:
- o Some functions that arise often in CS
- o Comparing the size of infinite sets

Announcements:

- o Dog day next Tuesday! BYOD.

Review

Domain. Co-domain. Range.
Injective (1-1) and surjective (onto) and bijective.

Notation: Sometimes you might want to show that f takes x to y, a to $2a$, etc. Don't use a $\rightarrow$symbol for that; write $x \mapsto y$, $a \mapsto 2a$. With surrounding English, this reads ok. But saying a $\rightarrow$2a definitely does not.

Some computer scientists like to denote functions by "**lambda expressions**"
To say that f is the function that maps x to x^2 we write
$f = \lambda\, x.\, x^2$

Here x is just a formal variable;
The domain is not mentioned explicitly

Functions don't have to be defined on numbers, of course; eg,

$|\,.\,| \;:\; \Sigma^* \rightarrow \mathbf{N}$
hd(x) = the first character of the string x, or ERROR if $x = \varepsilon$
tl(x) = all but the first character of x (and ε when $x = \varepsilon$)?
dim(A) = the dimensions of the matrix A, regarded as a pair of natural numbers

Functions can take any number of arguments – which we think of as forming the cross product.
Example: max: $\mathbf{N}^2 \rightarrow \mathbf{N}$

Functions can have domains that are complex sets,

max: $\bigcup_{i \in \{1,2,\ldots\}} \mathbf{N}^i \rightarrow \mathbf{N}$

δ^*: $Q \times \Sigma^* \rightarrow Q$

Formally, the domain is the cross product, but we don't routinely write things like $\delta^*((q, x))$; we write $\delta^*(q, x)$, understanding the function to operate on the pair.

It is also common, for some function, to switch to infix notation: $a+b$, rather than $+(a,b)$ (or, even worse, $+((a,b))$.

Function composition

$f \circ g$
$f: A \to B,\ \ g: B \to C$

then $(g \circ f) : A \to C$ is defined by
$(g \circ f)(x) = g(f(x))$

Kind of "backwards", but fairly tradition. Some mathematicians (eg, in algebra) will reverse it,
$(x)\ (f \circ g)$ "function operates on the left"

Inverse of a function

If $f(x) = y$ we say that x is a **preimage** of y
Does every point in the codomain have a preimage?
No, only points in the image.
Does every point in the image have **one** preimage?
No, only if it's an injective function
Does every point the in the domain have an image?
Yes, that's required for being a function.
Might it have two images?
No, only one.

If you do have a **bijective** function $f: A \to B$ then the function $f^{-1}: B \to A$ is well defined:
$f^{-1}(y)$ = the unique x such that $f(x) = y$.

Example: $f(x) = \exp(x) = e^x$
Draw picture.
What's the domain? **R**
What's the range / image ? $(0, \infty)$
Is it 1-1 on this image? YES

What's it's inverse? $y \mapsto \ln(y)$

Some important functions in CS

$\lfloor x \rfloor$ – define this.
$\lceil x \rceil$
$a \bmod b$
gcd (a,b)
// Calculating this: Assume a ≥b. If b = 0 then return 0. Else return gcd(b, a mod b).
a mod b ≤ a/2. (If b ≤ a/2, then a mod b ≤ a/2; if b > a/2 then a mod b = a – b ≤ a/2
$|x|$
2^x, e^x, a^x
lg, log, ln, $\log_b(x)$
$n!$
min X
max X -- *talk about what the domain of min and max are, and when these function are well defined.*

*Talk about the term **partial** (vs total) function*
gcd (*a,b*) = gcd(b, a mod b)

Proposition [Biggs, p. 35]: *Every nonempty $X \subseteq \mathbf{N} = \{1, 2, \ldots\}$ has a minimum.*
Proof. Let $P(n)$ = "every subset X of **N** containing n has a least number." Since X is nonempty, it suffice to show $P(n)$ for all $n \geq 1$.
Induction:
Basis: $P(1)$ is true because 1 is the minimum element of **N**.
Inductive step (strong induction). Suppose P(1), …, P(k) is true; must show P(k+1). So $k+1 \in X$.
Case 1: for all $x \in X$, $x > k$. Then $k+1 = \min X$.
Case 2. for some $x \in X$, $x \leq k$. By inductive assumption, X has a least number.

```
Review properties of logs:  // forgot to do in class
   log(ab) = log(a) + log(b)
   log_a(b) = log_c(b) / log_c(a)
   e^ab = (e^a)^b
   a^x a^y = a^{x+y}
Draw picture of y = lg(x)
```

Equicardinal sets

Sets A and B are **equicardinal** (or **equinumerous** or **equipotent**), written |A|=|B| or A~B, if there exists a bijection π: A→B.

Claim: this is an equivalence relation.

T/F: There is a bijection from A to B iff there is a bijection from B to A)

A set is **finite** if it is empty or equipotent with {1, …, n} for some natural number n
A set is **infinite** if it is not finite.
A set is **countably infinite** if it is equipotent with **N**.
Write $|A| = \aleph_0$
That symbol is called a **cardinal number**.
If $|A| = \aleph_i$ then $|\mathcal{P}(A)|| = \aleph_{i+1}$

So the numbers you know about are 0, 1, 2, …. , $\aleph_0$, $c = \aleph_1$, $\aleph_2$, …

Use |A|<|B| if there is an injection but no bijection from A to B.

Theorem [Cantor] $|A| < |\mathcal{P}(A)|$

Theorem [Schroeder-Bernstein] If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

Examples:
- {0,1, …} ~ {1,2, …}
- Show that the natural numbers and the integers are equicardinal
- Show that the rationals and the integers are equicardinal
- Infinitely many hotel rooms, room 1, room2, … .

In comes a new customer. Can you accommodate him (perhaps with a bit of inconvenience to existing customers?
Yes, shift everyone over. Showing a bijection from **N** to **N** ∪ {new}.

- Same but now infinitely many new customers arrive, new1, new2, …
  No problem: $n \mapsto 2n$ and we slot the new customers in at the odd positions.
  Show how to write it.
- Strings and numbers

Real numbers – can't be done. Let us now show this.

Diagonalization

- Prove that the set of **reals** is not countable. Focus on numbers in [0,1], Change chosen digit d to d+2 mod 10 along the diagonal.
- Prove that the set of **languages** over {0,1}* is **not** countable.
  Cor: there are languages that no computer program can recognize. (didn't get to this)
- Prove **Cantor's theorem (didn't get to this).**

These proofs – really the same proof – illustrate diagonalizatoin.
Used to prove Cantor's theorem, above, as well:

Proof of Cantor's theorem, from Wikipedia [Cantor's Theorem]: To establish Cantor's theorem it is enough to show that, for any given set *A*, no function *f* from *A* into the power set of *A*, can be surjective, i.e. to show the existence of at least one subset of *A* that is not an element of the image of *A* under *f*. Such a subset is given by the following construction:

$$B = \{ x \in A : x \notin f(x) \}.$$

This means, by definition, that for all *x* in *A*, $x \in B$ if and only if $x \notin f(x)$. For all *x* the sets *B* and *f*(*x*) cannot be the same because *B* was constructed from elements of*A* whose images (under *f*) did not include themselves. More specifically, consider any $x \in A$, then either $x \in f(x)$ or $x \notin f(x)$. In the former case, *f*(*x*) cannot equal *B* because $x \in f(x)$ by assumption and $x \notin B$ by the construction of *B*. In the latter case, *f*(*x*) cannot equal *B* because $x \notin f(x)$ by assumption and $x \in B$ by the construction of *B*.

Thus there is no *x* such that *f*(*x*) = *B*; in other words, *B* is not in the image of *f*. Because *B* is in the power set of *A*, the power set of *A* has a greater cardinality than *A* itself.

The continuum hypothesis [Wikipedia entry)

The continuum hypothesis (CH) states that there are no cardinals strictly between $\aleph_0$ and $2^{\aleph_0} = \mathfrak{c}$, the cardinality of the continuum (the set of real numbers). The generalized continuum hypothesis (GCH) states that for every infinite set *X*, there are no cardinals strictly between $|X|$ and $2^{|X|}$. The continuum hypothesis is independent of the usual axioms of set theory, the Zermelo-Fraenkel axioms, together with the axiom of choice (ZFC).